REMARKS

Claims 1-17 are currently active.

The Examiner has rejected Claims 1-4 and 9-16 as being unpatentable over Olson in view of Ballardie and Schneier. Applicants respectfully traverse this rejection.

Olson is a centralized peer-to-peer network, exactly the type of network from which applicants distinguish themselves. Applicants' claimed invention is a decentralized trusted peer-to-peer network. As stated in the background of the invention, on page 1, lines 24-27, of the above-identified patent application, trusted peer-to-peer networks have relied on a centralized process to establish a trusted peer-to-peer network, in contrast to applicants' decentralized claimed invention.

In a centralized peer-to-peer network, a central host device basically controls the interactions of the other devices in the network. In contrast, in a decentralized peer-to-peer network, each device operates essentially independent of all the other devices. The former is the structure of Olson, while the latter is a structure of applicants' claimed invention.

Olson, being a centralized peer-to-peer network, can be seen from the teachings in Olson that the host client assigns the application session a name and password, and can set

settings and operating criteria for the session, such as the maximum number of players permitted. The host client also coordinates and controls the addition of new clients into the application session. It is also the responsibility of the host to allocate unique identifiers to the client admitted into the application session, and to allocate identifiers to any players and/or groups created by other clients. See column 6, lines 50-60. Olson teaches that the host client is the first client in the application session, and is the client that will be responsible for admitting new clients into the session. See column 6, line 67 through column 7, line 3. Olson teaches that the host will typically assign a name for that particular session, and will then entertain requests from other clients on the network to be admitted into that application session. Other clients on the network 12 who are interested in participating in an application session may utilize available network protocols to seek out an existing host client. The client must request admission of the host for admission to the application session. See column 7, lines 10-16. Olson teaches that the host client will monitor and coordinate the admission of network connected clients seeking to participate in the application session. See column 7, lines 20-23. The host client processor monitors whether any network connected clients are requesting admission into the application session created by the host client. See column 7, lines 25-28. The host will admit the client into the application session depending on certain predefined criteria. See column 7, lines 33-36. If any applicable criteria are not met, the host client processor will deny access to the requesting client and return to the main section of the program code. If the admission criteria are met, the host client will permit the client into the

application session by performing a series of functional steps beginning at program step 42 of figure 2b. See column 7, lines 45-50.

Consequently, it is very clear from these teachings that the host client is taught to control who is admitted into a session and who is not, with the client itself totally subject to the control of the host device. Olson is a centralized network.

In contrast, applicants' claimed invention is specifically "a decentralized trusted communications network". The limitation "decentralized" in and of itself distinguishes over Olson and the applied art of record. However, to further make clear this distinction, Claim 1 has been amended to include the limitation that "a second computer either accepting or denying the public key in regards to joining the decentralized trusted network". This teaching does not exist in Olson. This is because Olson teaches that the client must request admission to the host client. Thus, this is the opposite of applicants' claimed invention. In applicants' claimed invention, it is the second computer that has control over whether it will become part of the network, while in Olson, it is the host client that has control over whether or not the client will be allowed entry into the session. In other words, the client would never request admission into a session and then once given admission, turn it down. Consequently, Olson actually teaches away from applicants' claimed invention because Olson teaches a centralized network and teaches that the client must receive permission from the host client, while in

applicants' claimed invention, there is a decentralized trusted network where the second computer has control whether it is going to enter the network or not.

In the Office Action, on page 3, the Examiner refers to column 6, lines 29-41 of Olson for teaching the limitation of "a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communication network with at least 2 of the n-users computing devices through which digital signals are shared". Referring to column 6, lines 29-41, it simply states that each client maintains its own copy of application data throughout the application session. The data is stored in the client's storage medium at elements 20, 22 and 24. Each of the plurality of clients can communicate with one another via the network 12 in ways that are well known in the art. Thus, when a client changes its application data, i.e. effects some change to the game state, that change is communicated to the clients in the application session by way of a state update packet sent to each client via the particular network facilities being used. That is all that column 6, lines 29-41 teaches. There is no discussion of a decentralized communication network.

In fact, continuing a review of the teachings of Olson, at column 6, line 42 states that a client has the option of either hosting a new game application or joining an existing one. When a client initiates a new game application system, that client is referred to as the host client. It is a host client that is responsible for managing the environment under which the distribution of application data between the client participating in the application session

takes place. For example, the host client can assign the application session and name and password, and can set settings and operating criteria for the session, such as the maximum number of players permitted. The host client also coordinates and controls the admission of new clients into the application session. It is also the responsibility of the host to allocate unique identifiers to other clients admitted into the application session, and to allocate identifiers to any players and/or groups created by other clients. See column 6, lines 42-60. This additional language taught by Olson clearly identifies a centralized communications network, as has previously been explained above. Again, to reiterate, Olson teaches a system for gaming that requires a centralized communications network where the host client has complete control over the parameters of the game and who can play the game. Applicants' claimed invention is a decentralized communications network that is not taught or suggested by Olson.

Olson does not teach a trusted member list. A table of unique identifiers is not a trusted member list, as the Examiner suggests on page 3 of the Office Action.

Referring to Ballardie, there is disclosed scalable multicast key distribution. As the title suggests of Ballardie, the teachings are focused on multicast, and how to provide secure multicast in an ever expanding network. In other words, the technique is scalable to a network that has routers that are added to it. Applicants respectfully emphasize the fact that the teachings of Ballardie have to do with multicast. Multicast is a well-known, well-defined

technique where a signal from a source node or host is repeated and distributed to many destination nodes throughout a network without necessarily the need for an MCU. Multicast is a one directional process in terms of the signal that is being multicast. The whole focus of Ballardie is in regard to multicast and how a connection is formed to distribute that signal from the host to the destination nodes securely.

The teachings of Ballardie regarding multicast have nothing at all to do with a decentralized or a centralized network. Ballardie teaches how to distribute a token from a host H to the core router C which, as shown in figure 1, is the key distribution center for the multicast signal to be distributed along the branches of the tree. It is taught on page 7 of Ballardie, the host H first contacts the router A to send a join request to router B, which includes its own unsigned token and the token of H and sends the request to the best next-hop on the path to the core C; the best next hop is router B. B verifies these join requests and then B repeats the aforementioned process except the join is sent from B to C. C authenticates B's join request. Once B and A have been verified, C forms a group access package which includes a token in an encapsulated joined acknowledgment. Two pairs of keys are included in the group access package, one for the originating host, and one for the next hop router to which the join acknowledgment is destined. See page 8 of Ballardie. The group access package is then sent back to B and from B to A. From A the key is set to H thus forming the entire path along which the signal is to be multicast from H is to be sent. If paths and nodes

fail, a new route for the core is gleaned as normal from the underlying unicast routing table, and the re-joining process occurs in the same secure fashion. See page 9 of Ballardie.

It is respectfully submitted that is all that Ballardie teaches. Ballardie does teach how to distribute a key to nodes of a path. However, Ballardie does not teach a decentralized network of any type where each computing device can communicate with all the other computing devices on the trusted peer-to- peer network. In a multicast path, the source node can communicate with all the destination nodes, but the destinations nodes cannot communicate with all the other destination nodes. The description of how the keys are passed from one node to the other only shows how one node communicates with another node along the path back to the source node. There is no teaching or suggestion of how to communicate from the destination node the key to another destination node. It is not necessary to do so, because in multicast the direction of the signal flows only one way and all that needs to happen regarding the key, is that it is distributed to all the nodes in the path. Furthermore, there is no teaching of a trusted member list. Accordingly, Ballardie does not add anything at all to the teachings of Olson to arrive at any other claims, as amended, of applicants.

Furthermore, there is no reason why one skilled in the art would combine the teachings of Olson with the teachings of Ballardie to arrive at applicants' claimed invention. Neither Olson nor Ballardie recognize or solve the problem of applicants' claimed invention solves. As explained above, Olson is focused completely on gaming over a network, while

Ballardie is simply focused on the multicast of a key for distribution purposes in an ever expanding network. In gaming over a network, Olson specifically teaches the host controls who can participate in the game. In a game over a network, you would never have an ever expanding network, which is what Ballardie deals with. There is no reason why Olson would have any need or use for the teachings of Ballardie, and vice versa. There is no reason why anyone skilled in the art would have any reason to combine the teachings of Ballardie with the teachings of Olson, let alone to somehow or other arrive at applicants' claimed invention.

In addition, patent law requires that teachings cannot be taken out of context in which they are found. The context of Olson is gaming and the context of Ballardie is multicast. These contexts cannot be ignored.

Referring to Schneier, there is taught a pretty good privacy which is a freeware electronic mail security program. It is respectfully submitted that because pretty good privacy is an electronic mail security program, it is non-analogous art to applicants' claimed invention, which has to do with a sharing of digital signals between the host computer and at least 2 of the user computing devices.

Besides the fact that Schneier is non-analogous art, Schneier also teaches that every user generates and distributes his own public key. See paragraph 1, page 585. Claim 1 has the limitation "the host computer sending a public key to a first of the 3 user computing

devices and the first user computing device sending the public key to a second of the 3 user computer devices and a third of the three user devices . . . each user computing device knows and can communicate directly with all the other user computing devices and the first computing device on the trusted peer to peer networks since the host computing device and all the other user computing devices have the public key". That is, the host computer and all the user computing devices have the same public key. In patent law by referring to "the" key, it is understood to mean the same key.

Schneier does not teach or suggest that the same key, "the public key" is utilized by each user so that they all can communicate with each other. From the very specific example that Schneier provides, Alice gives her public key to Bob. Bob knows Alice so he signed her public key. He then gives the signed key back to her and keeps a copy for himself. When Alice wants to communicate with Carol, Alice sends Carol a copy of the key Bob signed. Carol, who already has Bob's public key (she got it at some other time) and trusts Bob to certify other people's keys, verifies the signature on Alice's key and accepts it as valid. Bob has introduced Alice to Carol. From this example, it is clear that there is Alice's public key, and Bob's public-key. These are different keys. Thus, in order for Bob, Alice and Carol to communicate with each other, each user must generate and distribute his own public key, specifically as Schneier teaches. Thus, Schneier teaches to use different public keys for the users to communicate with each other, not the same key.

Furthermore, this distribution procedure taught by Schneier requires every user to give their own keys to every other user. There is no indirect distribution of keys as is found in the claimed invention. This is in direct conflict with the limitation of Claim 1 wherein the host computer sends a public key to a first of the 3 user computing devices and the first user computing device sends the public key to a second of the 3 user computing devices and a third of the 3 user devices. This distribution procedure is much simpler than the procedure taught by Schneier, and insures the ultimate purpose of applicants' claimed invention is reached, that the host computing device is able to communicate directly with each of the user computing devices so that the digital signals are shared securely between the host computing device and the 2 user computing devices. Besides the fact that Schneier is teaching only in regard to e-mails, only users that have all shared their own public key with all other users can they communicate with each other. In Claim 1 of applicants, the host computing device sends out the public-key to the first user computing device who then sends it on (indirect distribution) to the second and third user computing devices for the second and third user computing devices to then be able to communicate with the host computing device. Furthermore, Schneier does not teach or suggest a trusted member list.

Moreover, from the above discussion, it is clear that the only reason for one skilled in the art to even attempt to combine the teachings of the applied art of record, is the use of hindsight. This is not patent law. It is respectfully submitted the Examiner is using the limitations of applicants' claimed invention as a roadmap to find the various limitations in

disparate references, and supposedly having found them, concluding that applicants' claimed invention is arrived at. This, too, is not patent law. Schneier does not add anything to the teachings of Olson and Ballardie in relevant part in regard to the limitations of Claim 1, and Claim 1 is patentable over the applied art of record.

Accordingly, the applied art of record fails to teach or suggest a decentralized trusted communications network. Furthermore, the applied art of record does not teach or suggest a second computer either accepting or denying the public key in regards to joining the decentralized trusted network. Claim 1 is patentable over the applied art of record. Claim 2 is patentable for the reasons Claim 1 is patentable.

Claims 3-8 are dependent to parent Claim 2 and are patentable for the reasons Claim 2 is patentable. Claims 9 to 12 are dependent to parent Claim 1 and are patentable for the reasons Claim 1 is patentable.

The Examiner has indicated that Claims 5-8 would be allowable if rewritten with the limitations of their base claim on any intervening claims. Claim 17 is Claim 5 rewritten as such.

Claims 13-16 have the limitation of a "decentralized peer-to-peer network" and are patentable over the applied art of record.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 1-17, now in this application be allowed.

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

10/29/08
Date

Ansel M. Schwartz
Registration No. 30,587

Respectfully submitted,

By _____

Ansel M. Schwartz, Esquire
Reg. No. 30,587
One Sterling Plaza
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
(412) 621-9222

Attorney for Applicants